



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

GCWN Practical Assignment Version 3.1

Option 1: Design a Secure Windows 2000 Infrastructure

Submitted July 25, 2003 by Kris Wicks

© SANS Institute 2003, Author retains full rights

Table of Contents

Overview	1
Company Description of GIAC Enterprises.....	1
Network Design and Diagrams	3
Server assumptions.....	3
Client assumptions	4
Server naming conventions	4
Domain Controllers.....	5
Web Servers.....	5
IIS Server Configuration	6
Email Servers.....	7
File Servers	7
SQL Servers.....	8
Subnetting.....	8
Internet connectivity	8
Packet Filtering	8
Connectivity to remote sites	9
Active Directory Design and Diagrams	16
Overview.....	16
Domains.....	17
Sites	18
Site Replication	18
Organizational Units	19
OU Design and Diagram	20
FSMO Roles	21
FSMO Role Locations	23
Group Policy and Security	23
Basic Group Policy Implementation.....	23
Group Policy Overview	23
Group Policy best practices	24
Default Domain Policy	25
Default Domain Controller Policy	27
Additional Group Policies	29
R&D.....	29
R&D Servers	31
Additional Security measures.....	33
Physical Security.....	33
User and workstation naming conventions.....	33
Password Reset and Privileged Resource Access.....	34
Wireless and VPN access	34
Certificates.....	35

Overview

This document describes the secure Windows 2000 Active Directory and network infrastructure of GIAC Enterprises, a company involved with the design and manufacture of aftermarket performance parts on domestic vehicles. The document is laid out in four major categories:

Company Description – A brief overview of GIAC Enterprises business and operations.

Network Design – General infrastructure design for the company

Active Directory Design – Design and implementation of Windows 2000 Active Directory, including Domain and OU hierarchy and site implementation.

Group Policy and Additional Security – Basic group policy is identified and explained, as well as some additional security features not mentioned in other parts of the paper.

Company Description of GIAC Enterprises

GIAC Enterprises started rather unexpectedly over beer, in Kennewick, Washington when a conversation about cars turned into a lifelong obsession and a profitable company.

After several friends in the metal working program at a local vocational college turned to the disappointing fact that all the “hot rods” these days seemed to be modified from Japanese made cars, it was mentioned that the construction of cheap, high quality aftermarket performance parts could help change all that. The friends agreed to do something about it, and rather unlike most plans made over beer, this one sounded like a good idea the next day. And thus, in December of 1992, Greatly Improved Automotive Concepts was born.

From humble beginnings in the family garage of one of the company’s founders, GIAC has become one of the best known and most successful companies to produce domestic aftermarket performance parts in the US, earning over \$50 million in revenue last year. It currently only creates aftermarket parts for Ford Motor Vehicles’ cars, but has plans to widen their business to other domestic companies such as Generic Motors in the near future. While many customers have begun using the automated web ordering system, over 60 percent of GIAC’s yearly sales still come from customers working directly with their sales staff.

The main office is still in Kennewick, Washington. This location employs 500 people, all of whom use the computer daily for at least mail and the electronic timecard system. Out of the employees in this office, 100 are involved in

manufacturing, 50 are Research and Development, 250 are Sales and Marketing, 75 are Administration and Management, 15 are Financial and HR, and 10 are general IT staff. 30 members of the Sales and Marketing staff are a traveling sales force, constantly at car shows and visiting resellers.

The R&D department is comprised of the following two groups: The Electronic Enhancement team reverse-engineers the regulator chips found on newer vehicles in order to create special high-performance “mod-chips”. Some of their mod-chips can be connected to a PDA device and modified on-the-fly. The Mechanical Enhancement team experiments constantly with different alloys to create strong, lightweight racing components. The company is understandably concerned with keeping this information from their competitors, and has strong security requirements for the R&D group.

GIAC has two other locations, in Orlando and Los Angeles, which each contain 35 employees. These locations are strictly Sales and Marketing, and have increased company business revenue by over 20% in the five years that these branches have been opened. Five employees in each location are on hand to cover HR and Financial duties. Any hardware problems with PCs in these locations are handled by a local company, and all administration on servers and desktops is done remotely from the main office. These offices have been so beneficial to the company over the last few years that serious consideration is being put into the possibility of opening up other locations in New York and Las Vegas.

© SANS Institute 2003, All Rights Reserved

Network Design and Diagrams

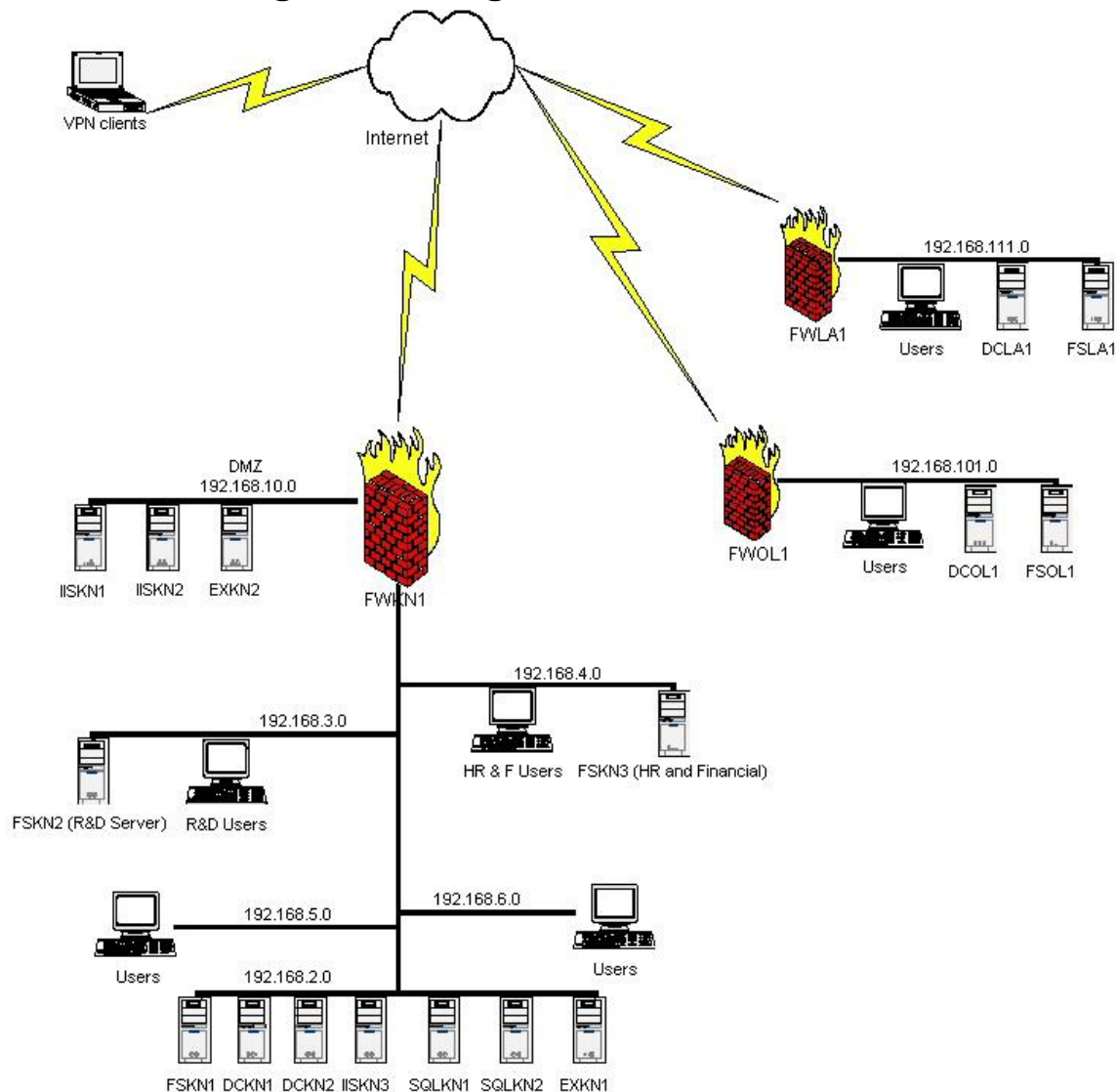


Figure 1 - Network Design

Server assumptions

The following should be assumed of all servers on the GIAC domain unless otherwise stated.

- All servers are running Windows 2000 Server SP3, and relevant patches are applied regularly.
- Symantec Antivirus is installed on all servers, and the signature files are updated weekly unless an urgent signature is released.
- Terminal Services Remote Administration mode has been enabled on all servers for ease of administration.

- All nonessential services have been disabled. All essential services have been set to automatically restart if failure occurs.
- All drives are running NTFS.
- All servers have the system state and any data backed up fully every Friday night, with incremental backups every Monday and Wednesday. A copy of the full backup tapes for the last two months is kept in a vault at a nearby bank.
- All servers require IPSec connections from client computers, running at least AH.

NetBIOS over TCP/IP is not disabled on internal servers, because the backup software currently used by the company requires it. External machines, such as the web servers, do have this functionality disabled.

Client assumptions

Clients are not quite as standardized as servers. Client hardware is updated on a three year lifecycle, with the oldest client machines currently being Dell GX110s running 650MHz PIII's and 256MB RAM.

- Clients run Windows 2000 Pro with SP3 or Windows XP Pro with SP1 and all applicable patches. All Win9x clients were retired when the site went to Active Directory. There is a project underway to roll out XP to the entire site, but will take some months to complete.
- End users do not have Admin rights to their systems.
- A startup script applies patches and service packs to clients, as well as any application updates.
- Clients are running Symantec Antivirus as their virus scanning software, and the signature files are updated weekly unless an urgent signature is released.
- All unnecessary services have been disabled, and no client runs IIS, Telnet or FTP services.
- NetBIOS over TCP/IP is disabled.

Server naming conventions

Although GIAC has managed to keep the number of servers to a fairly small number, they have deemed it important to be able to determine what the primary function and location of a server is just by looking at the name.

The server functions are as follows:

DC = Domain Controller

FS = File Server

EX = Exchange Server

PS = Print Server

AS = Authentication Server

RR = Routing and Remote Access Server
IIS = IIS Server
SQL = SQL Server
FW = Firewall or web proxy

The location designations are as follows:

KN = Kennewick, WA
OL = Orlando, FL
LA = Los Angeles, CA

The naming convention then, is simple: DCKN1, where DC is the server function, KN is the location designation. The number at the end is a simple identifier in case there is more than one of a particular server in any one location.

Domain Controllers

There are two Active Directory (AD) Domain Controllers (DC) located in the primary site, for fault tolerance and FSMO distribution purposes. There is one DC in each child site, as is required to create remote sites. Due to the relatively small number of users in each site, there are no load issues with any of the DCs.

Each DC is also a DNS server. Since all win 9x clients have been retired, there is no requirement for WINS name resolution.

AD Integrated DNS is set up on the DCs with secure dynamic updates required, and zone transfers are only allowed to trusted servers.

The option to secure cache against pollution is also enabled, which protects against cache poisoning by dropping any un-requested records returned when the DNS server requests a record from another DNS server.

The internal DNS servers are configured to forward unresolved names to the DNS server for GIAC Enterprises' ISP. This is a good idea, since the ISP's DNS server is already a hardened system.

Each DC has three disk sets. One with the Windows 2000 Server operating system running in RAID1 configuration, the other two running RAID5 and containing the SYSVOL and the logs, respectively.

Web Servers

GIAC has two external web servers, IISKN1 and IISKN2 running in the DMZ of the main location. The web servers are running Windows Load Balancing (WLB) for all web traffic. HTTP and HTTPS are both supported on these servers. These servers use Verisign certificates for SSL authentication with clients. They are published externally as www.giac.com.

There is also an internal web server IISKN3 at the primary site for employee info and the web-based timecard system. This server also supports HTTP and HTTPS communication. Since this server is for internal use only, a certificate has been granted for SSL authentication from the internal Issuing CA.

IIS Server Configuration

The IIS Lockdown tool is used on all IIS servers in order to secure them. The “Dynamic Web server” template is used, and URLScan is set to run under this template, as well. After this configuration, minor changes are made to the servers to modify them to comply with company requirements.

IIS Configuration

HTTP is enabled

FTP is enabled

SMTP is disabled

NNTP is disabled

ASP is enabled

Index Server Web Interface is disabled

Server side includes are disabled

Internet data connector is disabled

Internet printing is disabled

HTR scripting is disabled

WebDAV is disabled

Anonymous user system utility execute rights are disabled

Anonymous user content directory write rights are disabled

IISsamples virtual directory is removed

Scripts directory is removed

MSADC virtual directory is removed

IISadmin virtual directory is removed

IIShelp virtual directory is removed

URLScan “Dynamic Web Server” configuration changes

Allowed Headers

GET

HEAD

POST

Allowed Extensions

.asp

.cer

.cdx

.asa

.htm

.html

.txt
.jpg
.jpeg
.gif

The following executable files are removed from the %systemroot%\system32 directory and placed in c:\tools. The tools directory is not added to the path statement of the server.

- Cmd.exe and command.com. These are the Windows command console.
- Cscript.exe and wscript.exe. These are the Windows Script Host engines.
- Ftp.exe. Command line-based FTP.
- Net.exe and net1.exe. Command line-based computer management tool.

All webs have been moved from the drive containing the operating system, and the IUSR anonymous account has been explicitly denied access to that drive. File and Printer sharing is disabled on both external IIS servers, although it is enabled on the internal IIS server for ease of file upload.

Email Servers

The primary site has been recently upgraded to Exchange 2000 from Exchange 5.5. There is one Exchange server at the primary site, EXKN1. Employees at the child sites also have their mail stores on this exchange server, although complaints of slowness at peak times have caused the company to consider deploying exchange servers in the child sites as well, or increasing bandwidth.

There is an IIS server configured as an SMTP relay on the main site's DMZ. This is a standalone server which can only be administered from the IP addresses assigned to the Admin desktop systems. Although not an exchange server, the server name is EXKN2, and the box is published via the ISA server as mail.giac.com. Since this server only acts as a relay between the internal exchange server and the ISP's internet mail server, and users do not directly access this server, third-party POP3 services are not required.

File Servers

GIAC headquarters has 3 file servers, and each child office has one as well. One of the file servers at GIAC headquarters is used primarily for user data, while the other two are used for sensitive HR and financial data, and R&D development data, respectively. The HR and R&D servers require IPSec ESP, and are only available to certain security groups.

File servers have two drive sets. The first drive is for the operating system and is configured as RAID0. The other drive set is composed of 3 or more drives in a RAID5 configuration.

SQL Servers

The main GIAC site hosts three internal SQL 2000 servers, SQLKN1, SQLKN2, and SQLKN3. SQLKN1 stores contact information and sales data for the GIAC.com external website, while SQLKN2 stores internal databases for manufacturing, sales and marketing teams. SQLKN3 is maintained by HR and Financial for employee records not contained within Active Directory.

Subnetting

As depicted in the network diagram, the subnet configuration is fairly straightforward. All servers in the primary office—with the exception of the R&D and HR & Financial file servers—are on the 192.168.2.0 subnet. The internal interface of FWKN1 is on the 192.168.1.0 subnet, in order to provide some protection in case the ISA server is compromised, and incoming connections to RPC, RDP, SMB, and similar protocols from the ISA server are disabled on the router.

The R&D department is on 192.168.3.0 and the HR & Financial department is on 192.168.4.0. These departments are similar in their network configuration. Incoming SMB requests are disabled at the router, since the servers are maintained internally, and outside users do not need to connect to the servers. Most GIAC employees are on the 192.168.5.0 and 192.168.6.0 subnets, as there are too many machines to put on only one subnet.

Internet connectivity

The primary location in Kennewick has one firewall in a tri-homed configuration, FWKN1. It is configured as an integrated firewall and proxy server, and restrictive ingress and egress filtering policies are enabled on the ISA server, detailed in the following subsection.

The DMZ at GIAC headquarters is home to the GIAC.com external website, which allows both car enthusiasts and resellers sales access to the online catalog, and ability to order products directly from GIAC. Although they are a relatively small company employee-wise, their web site gets a decent amount of traffic. They have a cluster of two IIS servers with access to internal sales and accounts data.

The remote sites each have a single ISA integrated firewall and proxy server, FWOL1, and FWLA1.

Packet Filtering

Users must be authenticated on the domain in order to get external internet access, and can not get Web and FTP access from servers. A security group

containing all desktop computers on the site is applied to the Web and FTP rule sets.

The following is the configuration of FWKN1. FWOL1 and FWLA1 have similar though less complex configurations, due to the lack of published resources on the child sites.

Web and FTP access: Users on workstations are only allowed access to web content on ports 80 and 443, and FTP on port 23. This prevents trojans installed on client machines from accessing external computers over arbitrary port numbers, as well as keeping employees on task by blocking instant messengers and P2P applications.

Email Server filtering: the external email server on the DMZ has only port 25 open on the external interface for SMTP. This prevents any attackers from attempting exploits against anything other than this port externally.

Internally, Port 25 is open only to the IP address of the exchange server, and ports 23 for FTP and 3389 for RDP are open to the IP addresses of the administrators' desktop machines. FTP is used to transfer updates to this server, and administration is done using Terminal Services.

Web Server filtering: The external web servers have only ports 80 and 443 open on the external network interface for http and https traffic. Internally, like the email server, ports 23 for FTP and 3389 for RDP are open to the IP addresses of the administrators' desktop machines for transfers of patches and for remote administration. In addition, port 1433 is open to SQLKN1, in order to store or query customer information.

DNS: No internal DNS information needs to be available to outside sources, since all Internet traffic goes through the proxy servers. Outgoing DNS requests are allowed from UDP port 53, and there is no requirement for zone transfers.

VPN Connectivity: As mentioned in the next section, for ease of use and configuration, the VPN server is also the ISA server. Clients are allowed to connect on UDP 500 to perform Internet Key Exchange (IKE), and UDP 1701 for L2TP transmissions. Separate rules allowing IKE and L2TP between the remote offices' gateways are also configured, in case the primary rule needs to be disabled.

Connectivity to remote sites

The Los Angeles and Orlando sites send quite a bit of information back to the parent site, but most of the data is in fairly low-bandwidth documents and email.

Since traffic is so light, and the domain is small and requires few updates, there are no time restrictions on AD replication.

Up until recently the child sites had dedicated T1 lines to headquarters, but in an effort to cut costs, the dedicated T1's have been retired, and the child offices now communicate using a gateway-to-gateway VPN connection with the previously existing T1 connected to the internet. The child sites very seldom need to communicate with each other directly, so the only VPN connections are between the child sites and headquarters, although the VPN connections can perform hub-and-spoke type connections between child sites when necessary.

Gateway-to-gateway VPNs using L2TP over IPSec are created between the ISA servers at the home office and remote offices. This is an accepted and well-documented method detailed in Thomas W. Shinder's "ISA Server and Beyond". This is most easily done using the Local VPN Wizard, as shown below.

1. In the ISA admin console, right-click "Set up Local VPN Server". Select Next
2. Type in the name of the local office for the local network name, and the remote office for the remote network name, in this case, Kennewick and Orlando, respectively. Hit next

Local ISA VPN Wizard

ISA Virtual Private Network (VPN) Identification

The ISA Virtual Private Network (VPN) connection is identified by a unique name, based on the names of the two communicating networks or computers specified here.

Type a short name to describe the local network:

Kennewick

Type a short name to describe the remote network:

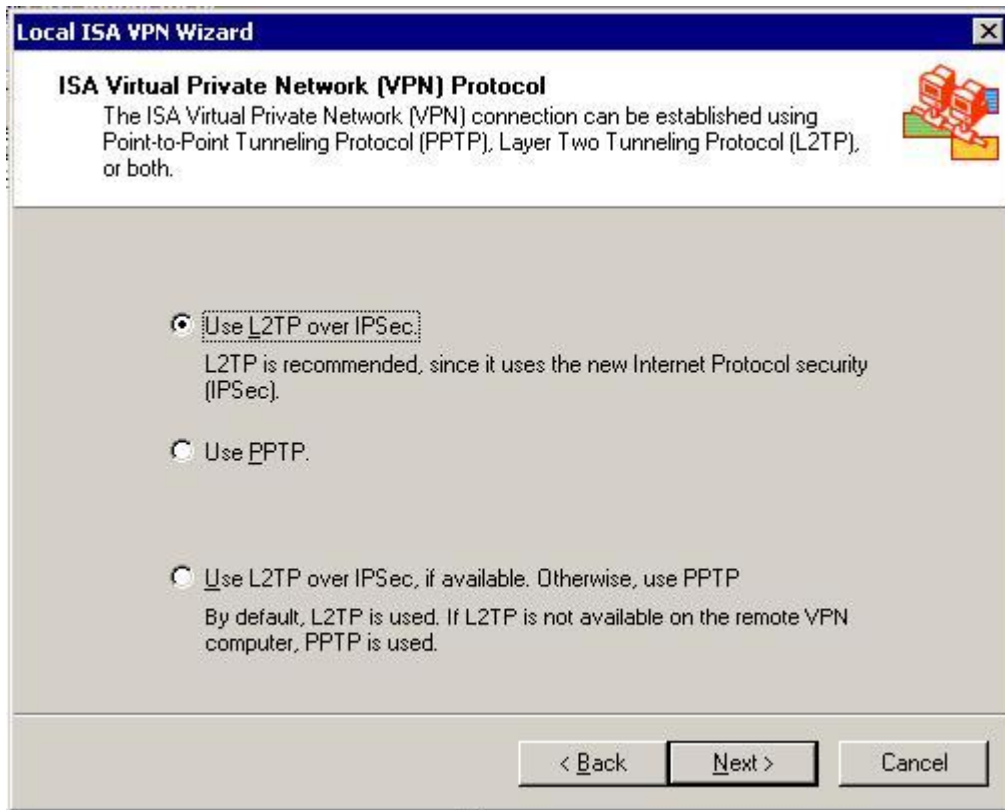
Orlando

The VPN connection will be identified by this name:

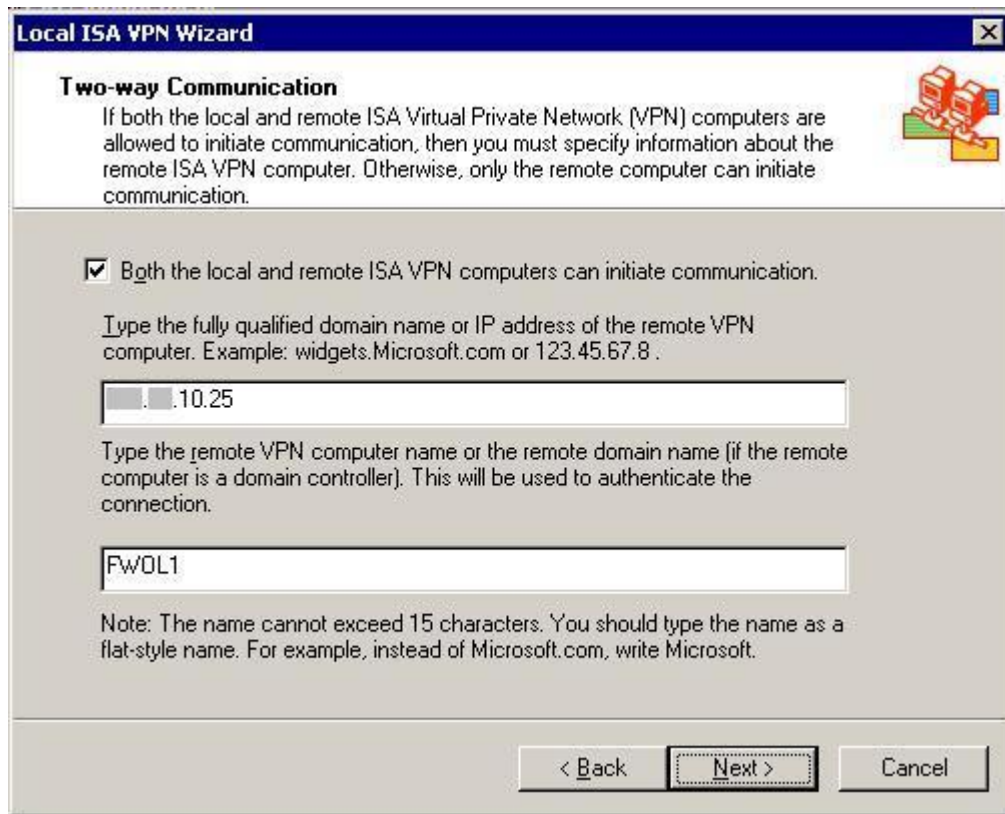
Kennewick_Orlando

< Back Next > Cancel

3. Select L2TP over IPSec as the VPN Protocol and hit next



4. Put a check mark in the box to allow either ISA server to initiate connections.
5. Type in the IP address of the remote ISA server's external network interface in the first box. Do not use the FQDN for the remote ISA server, to ensure safety against domain hijacking. Type the remote computer name in the second box.



Local ISA VPN Wizard

Two-way Communication

If both the local and remote ISA Virtual Private Network (VPN) computers are allowed to initiate communication, then you must specify information about the remote ISA VPN computer. Otherwise, only the remote computer can initiate communication.

☒ Both the local and remote ISA VPN computers can initiate communication.

Type the fully qualified domain name or IP address of the remote VPN computer. Example: widgets.Microsoft.com or 123.45.67.8 .

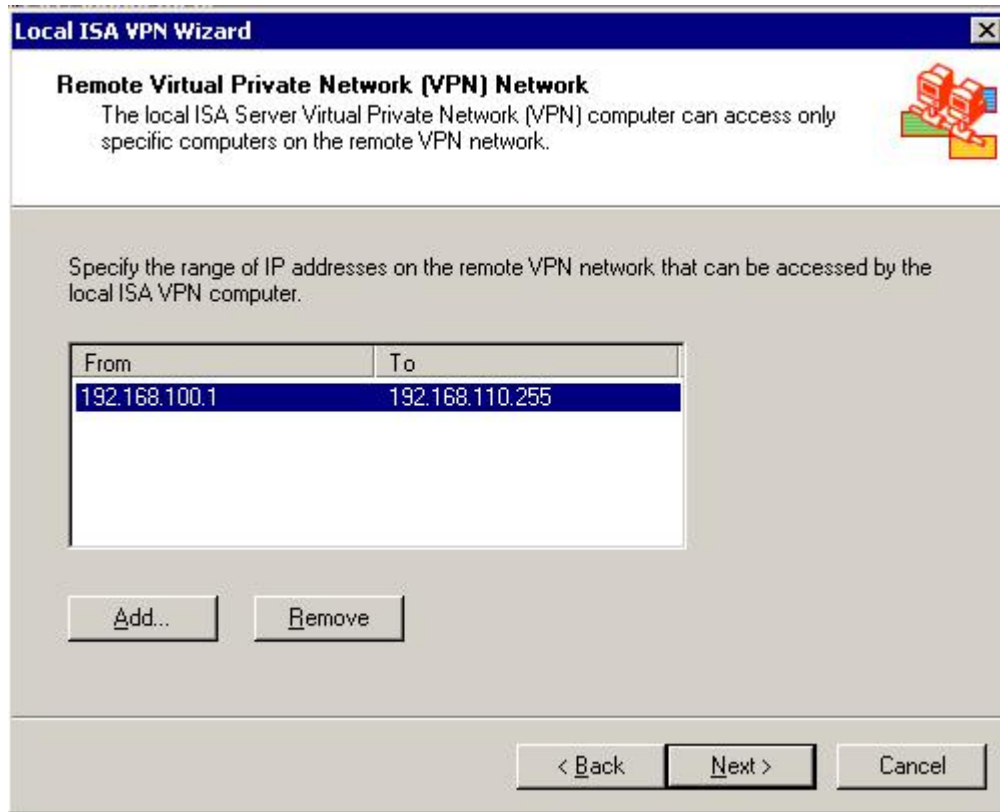
Type the remote VPN computer name or the remote domain name (if the remote computer is a domain controller). This will be used to authenticate the connection.

Note: The name cannot exceed 15 characters. You should type the name as a flat-style name. For example, instead of Microsoft.com, write Microsoft.

< Back Next > Cancel

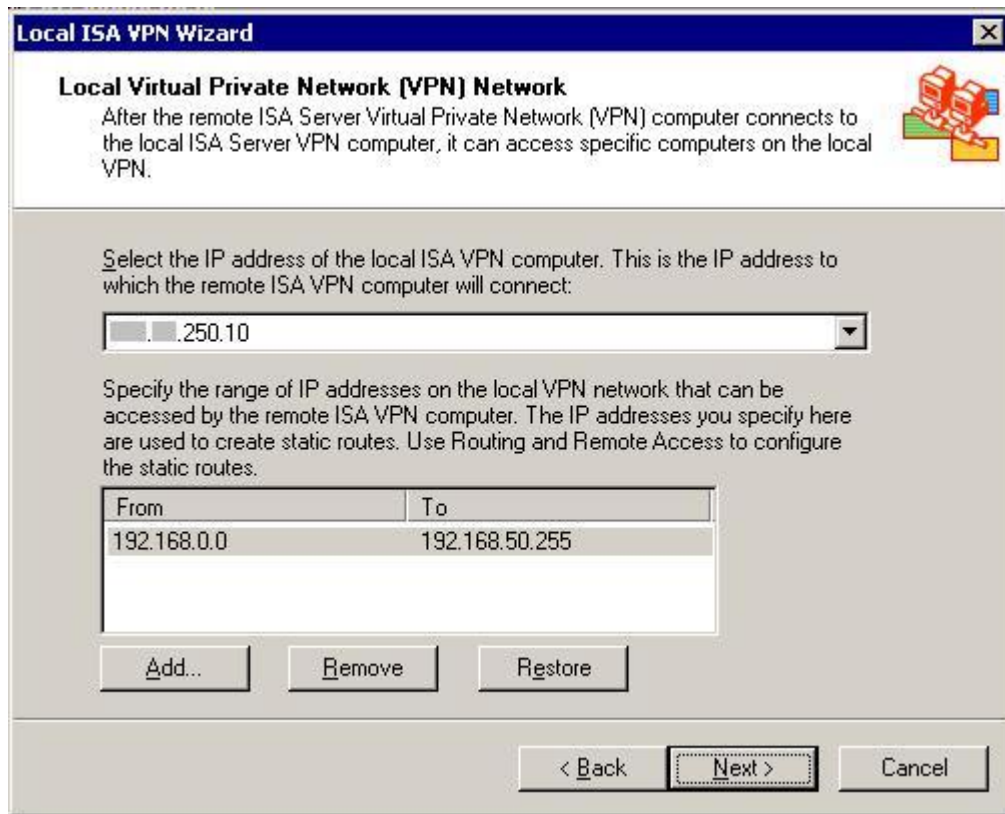
6. Enter the IP range accessible over the VPN connection. In this case, even though only two subnets are used at the remote site, this range is reserved for future expansion.

© SANS Institute



7. Select the external network interface of the ISA server, and enter the internal address range available to the remote site.

© SANS Institute 2003



Local ISA VPN Wizard

Local Virtual Private Network (VPN) Network

After the remote ISA Server Virtual Private Network (VPN) computer connects to the local ISA Server VPN computer, it can access specific computers on the local VPN.

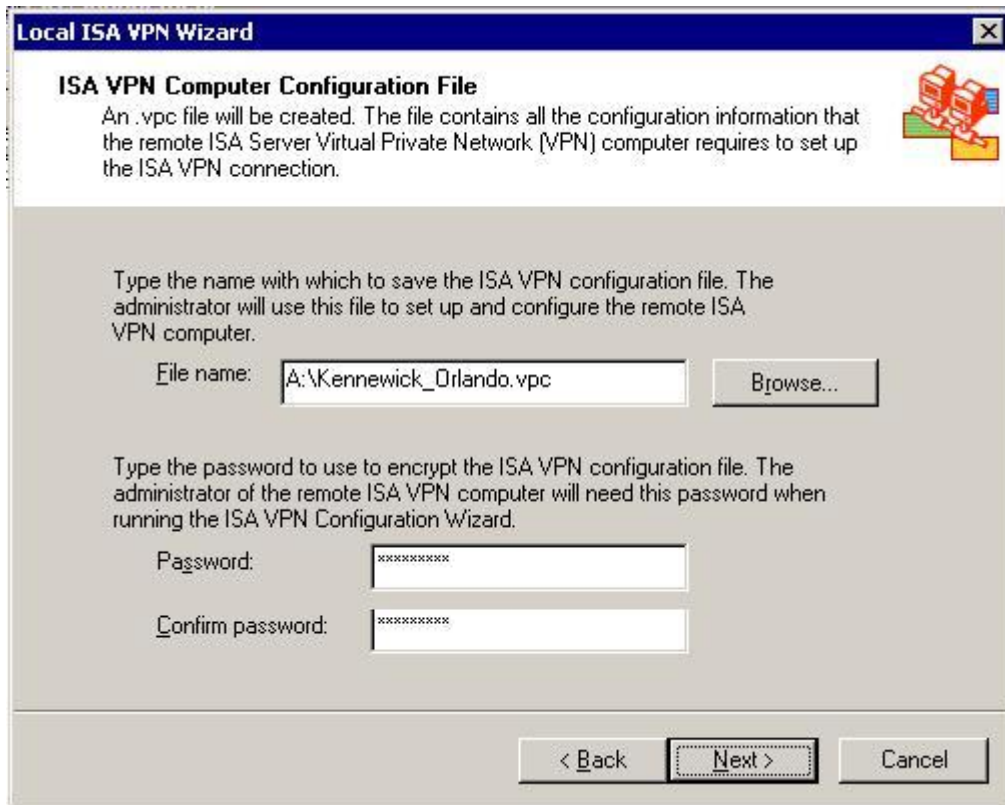
Select the IP address of the local ISA VPN computer. This is the IP address to which the remote ISA VPN computer will connect:

Specify the range of IP addresses on the local VPN network that can be accessed by the remote ISA VPN computer. The IP addresses you specify here are used to create static routes. Use Routing and Remote Access to configure the static routes.

From	To
192.168.0.0	192.168.50.255

8. Save the remote configuration file. This will configure everything required to make a connection with the local ISA server on the remote server.

© SANS Institute 2003



The image shows a Windows XP-style dialog box titled "Local ISA VPN Wizard". The main heading is "ISA VPN Computer Configuration File". Below this, a paragraph states: "An .vpc file will be created. The file contains all the configuration information that the remote ISA Server Virtual Private Network (VPN) computer requires to set up the ISA VPN connection." To the right of this text is a small icon of three computer monitors. The next section prompts the user to "Type the name with which to save the ISA VPN configuration file. The administrator will use this file to set up and configure the remote ISA VPN computer." It features a text input field with "A:\Kennewick_Orlando.vpc" and a "Browse..." button. The following section prompts for a password: "Type the password to use to encrypt the ISA VPN configuration file. The administrator of the remote ISA VPN computer will need this password when running the ISA VPN Configuration Wizard." It has two password input fields, one labeled "Password:" and the other "Confirm password:", both showing masked characters. At the bottom are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

9. Click finish on the final screen.

This process starts RRAS on the ISA server, and automatically configures the VPN connections, filters and user accounts necessary for a gateway-to-gateway VPN connection.

© SANS Institute 2003, Author

Active Directory Design and Diagrams

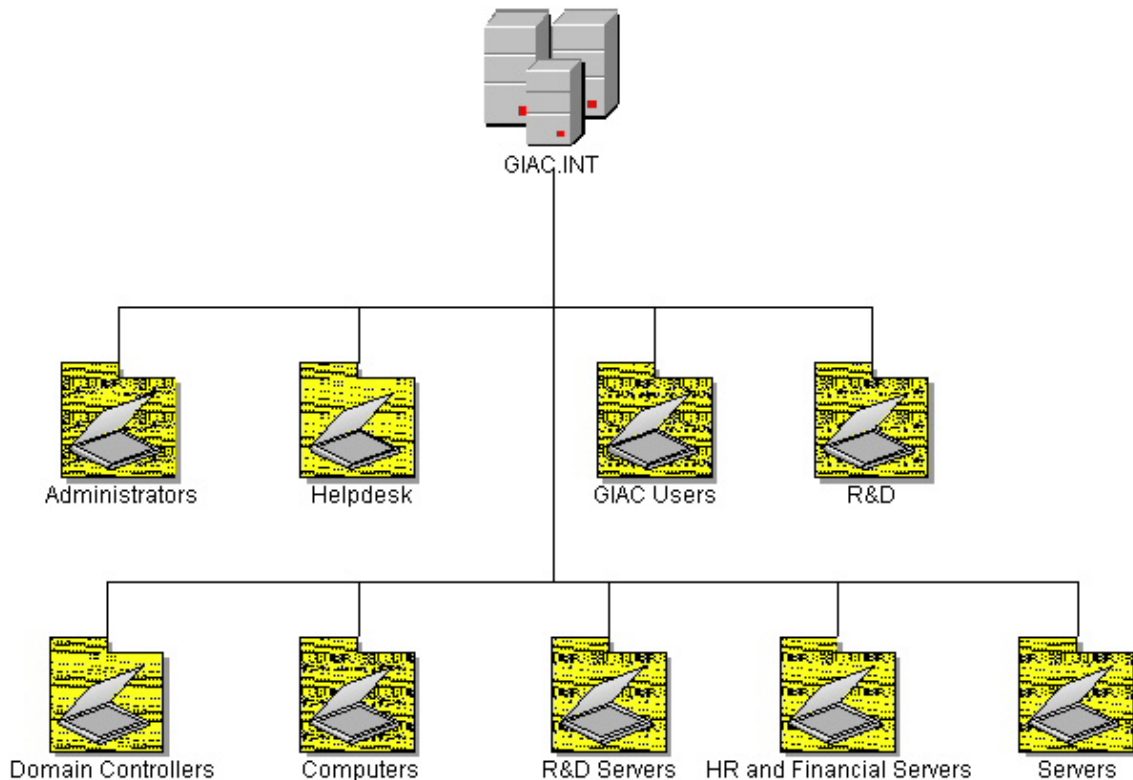


Figure 2 - Active Directory Infrastructure

Overview

AD is a central repository for user and computer accounts, groups, etc. GIAC takes it one step further. The GIAC Corporation chose to implement Active Directory as a central repository for all user data. Much of the HR data on a person is stored in their user account with special permissions associated to it. Since payroll information and SSN are not included by default in AD user accounts, special changes to the schema had to be made to accommodate many of these items.

The correct number of AD domain controllers to implement on the domain at each site was determined by utilization of the ADSizer tool. The Active Directory infrastructure for GIAC required the creation of only one forest, one tree, and one domain.

Active Directory was implemented in a manner which assures high availability and stability of the network. Security is second only to availability to this company, as a down network could be hundreds of thousands of dollars in lost revenue.

Domains

A domain is an administrative and security boundary for objects within Active Directory, meaning that policies applied to a domain apply only to that domain, and security applied to a domain only applies to users and objects of that domain. A Domain Admin of one domain is not a Domain Admin of another domain just because there is a trust between domains.

An AD domain uses multi-master replication. This allows changes in domain objects to be made on any DC, which are then replicated to all other DCs on the domain. Replication links are created between DCs on the same site automatically by the Knowledge Consistency Checker (KCC), which determines the best AD replication topology.

An Active Directory can consist of one or more interlinked domains. Unlike NT4.0 domains, an AD domain can have hierarchical structures, such as parent-child domain relationships. A child domain would have to have a contiguous DNS namespace indicating that it was a sub-domain of the parent. For example, a domain named XYZToys.com would have a child domain named abc.XYZToys.com. A relationship of this sort is called a Tree in AD nomenclature.

AD can also contain domains with non-contiguous DNS namespaces. For example, a company might have a top level domain named XYZToys.com, and another named ABCFarms.com. These can be joined in the AD as a Forest. While forest members do not need to be contiguous namespaces, all top level domains in AD must be at the same level. For example, XYZToys.com and sales.ABCFarms.com cannot both be top-level domains in an AD infrastructure.

Since GIAC decided to implement each location as an AD site rather than its own domain for the sake of simplicity, and has no current plan for expansion to foreign countries in the near future, they saw no reason to implement a multi-domain infrastructure.

There are several advantages to implementing a single AD domain over multiple domains. First and foremost is simplicity. There are no trusts and no inter-domain replication issues to worry about. It is easier to administer, as it is simpler to find user and computer objects, and a single domain model requires fewer DCs than a multi-domain model.

Early on, it was suggested that an empty domain should be created to enhance security, but this was abandoned in favor of more restrictive policy toward domain admin accounts. It was also suggested in planning that the R&D group should have their own domain in order to shield them from other users. After it was pointed out that access could be limited to fixed location by security groups, and using organizational units, domain admins could be removed from the local administrator group on clients/servers, and password policy would not be any

different due to the use of smart-card technology by the R&D staff, detractors to the single-domain model were finally silenced.

The domain was configured as GIAC.INT. Since this is an exclusively internal domain, the registered public domain name GIAC.com does not need to be used. An internal domain name which is not resolvable from a standard internet system makes it simple for users and Admins alike to determine whether a system is internal or external.

Sites

In NT4.0 days, it would have been necessary for GIAC to create multiple domains due to the disparate locations of the company. Active Directory sites make the creation of a single domain extent across large physical distance into a realistic option.

An AD site is a logical topological partition which receives sparse scheduled updates from the domain in different locations. While a site is a component of AD, it is not always specific to a domain. A domain can contain many sites in different locations, and a site can contain or partially contain several domains.

While the Knowledge Consistency Checker (KCC) can create replication links automatically between DC on a domain within a site, the KCC can not automatically create links between DCs in different sites.

Although connections need to be created by the AD architects, this is generally not a manual process. Sites are composed of one or more subnets and must contain a minimum of one DC. Subnets may not be shared between sites.

Site Replication

In inter-site replication, one DC is specified as a “bridgehead” server for each link. A bridgehead must be a Global Catalog server (GC). This server replicates with the other bridgehead server on another site. A DC can be bridgehead for multiple links, and there may be more than one bridgehead to the same site for purposes of fault tolerance. Once the bridgehead server has received data from another site, it replicates this data using intra-site replication. Intra-site and inter-site replication differ in several ways. In order to save bandwidth over slow links, inter-site replication is condensed to 10 to 15 percent of its original size. While this does save bandwidth, it imposes a processing load on the bridgehead servers. Processing load on the DCs is not a concern for GIAC, since 500 users do not put much of a load on the servers.

There are two replication methods available for inter-site replication; RPC and SMTP.

RPC: AD uses RPC over IP automatically for replication within a site. This method provides high-speed, efficient connectivity. RPC over IP is the default transmission method for inter-site transmissions and should be used in most cases.

SMTP: SMTP supports schema updates and global catalog replication between sites. It does not support functions such as FRS and so can not be used for intra-site replication. SMTP replication is most suitable for unreliable site links, or for sites which for some reason can not connect to the other sites directly.

Since GIAC uses VPN connections over T1s, replication using RPC over IP is the best choice. The replication schedule runs from 10 pm to 1 am every night, and from 12 pm to 1 pm every weekday, in order to minimize the effect of replication traffic on individual workers.

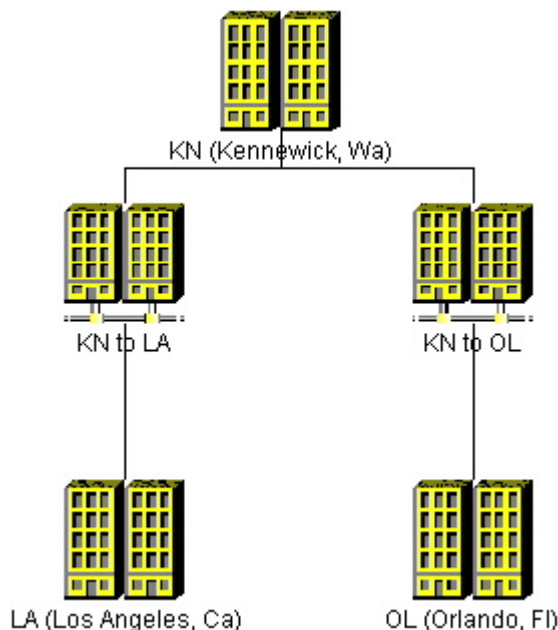


Figure 3 - Domain site links

Organizational Units

In designing organizational units (OU), several considerations should be taken into account: How much of the OU structure is based primarily by organization, and how much must be based on physical location? What is the minimum depth realistically attainable for the OU structure? OUs are primarily designed for two things: Logical organization of users, groups and computers, for permission delegation, and organization of resources for policy application.

How much granularity do you plan to implement in permission delegation? Least privilege is a good goal, but users have to know who to go to in order to get

accounts unlocked or groups modified, and it can be frustrating and confusing if these people are completely different for each OU. One of the concepts of OU usage is to nest similar groups under a primary OU. It is important to keep nesting in perspective. While it can be tempting from a political standpoint to implement an OU structure in a similar manner as an organizational chart, this is usually a bad idea. You do not want your OU structure to be re-created every time a reorganization of the company is planned.

Too much nesting can make it very difficult to find specific resources quickly, and it can make upkeep on group policy very difficult. It is generally smarter to set up OUs in as flat a structure as reasonable, and link GPOs to OUs.

Although it is possible to include users, groups, and computers in the same OU, this is not always a good idea. From an organizational standpoint, it is often much simpler to design group policy around OUs with either users or computers. Group Policy cannot be applied to security groups.

OU Design and Diagram

The default domain receptacles named “Users” and “Computers” are not true OUs in that policy cannot be applied to them individually; they only apply the default domain policy. GIAC uses the Computers OU only for workstations, but does not use the Users receptacle, and other OUs are created for general users.

Because there is no user policy assigned at the root domain, it is important to ensure that user accounts do not end up in the Users receptacle. GIAC has addressed this using two methods. The first is that the small group of account operators at the helpdesk who create new user accounts are explicitly denied the ability to create user accounts manually in any OU. They must use the User Account Manager (UAM) tool to create accounts, which only allows user accounts to be created in specific OUs. UAM runs under a service account which has user creation rights for all OUs on the domain, and has the added bonus of automating much of the user creation process by providing dropdown menus with default information. The second method is a script that runs on the domain controller every day which checks for new user accounts. It enumerates all user accounts in all OUs, and compares them against the list created the day before. If a new account has been created or moved, a message is sent to the Admins detailing the name and location of the new account.

The following table lists all OUs in the GIAC.INT domain. The right column of the table shows whether the OU is created under the root of the domain or within another OU. Built-in OUs are not specified in this list.

Organizational Unit	A child OU of	Contains
Administrators	Domain Root	Users and Groups
Helpdesk	Domain Root	Users and Groups

R&D	Domain Root	Users, Computers, and Groups
GIAC Users	Domain Root	Users and Groups
Servers	Domain Root	Computers
R&D Servers	Domain Root	Computers
HR and Financial Servers	Domain Root	Computers

The HR and Financial team and the Sales and Marketing team do not have their own OUs because the requirements they have for their computers are not significantly different from what the manufacturing team requires. User accounts for all three of these teams are located in the GIAC Users OU. There are also no separate OUs for the child sites, since there is no requirement for additional policy, and object creation/modification are all handled by the helpdesk and administrators in the main office.

The Administrators and Helpdesk OUs have less restrictive policies than the GIAC Users, and these OUs have been locked down so that only administrators can modify the objects within the Administrators or Helpdesk OU.

The Domain Admins group is added as local administrators on all workstations and servers, except for those in the R&D and R&D Servers. These OUs have highly restricted policy and management requirements, and have a separate administrator who is part of the R&D group.

FSMO Roles

Microsoft has made much ado of Windows 2000 AD being a multi-mastered infrastructure. While it is true that all primary functions, such as account creation, GPO and OU creation and modification, and many other functions can be done from any 2000 DC and replicated to other DCs, there are several background services which must be unique to a particular DC and which must run in order for the AD to remain in a healthy working order. These are labeled collectively as Flexible Single Master Operations (FSMO). A brief description of FSMO roles and locations is provided below.

Schema Master: The schema master holds the master copy of the AD schema.

The schema contains the master list of all object types and attributes in AD, such as user and computer accounts. The DC hosting the schema master role is the only one which can modify the schema. Any updates are replicated to the other DCs in the domain. Since all DCs have a full copy, and the schema is very rarely updated on the production AD, a short outage of this FSMO role should not cause any noticeable issues.

There is one Schema Master per forest.

Domain Naming Master: The domain naming master is responsible for updating and maintaining and modifying the domain namespace. This role is used primarily for adding and removing domains. In complex infrastructures, the

domain naming master should always be a global catalog server or failures in creation of child domains can occur (Q315850).
There is one Domain Naming Master per forest.

PDC Emulator: The PDC Emulator has many important functions. It acts as a PDC if any NT4 BDCs are still on the network, as well as managing password changes for NT and 9x clients. It also minimizes replication latency for password changes. When a password is changed on an AD domain, the DC on which the password is changed immediately forwards the password to the PDC Emulator. In larger organizations it can take a while to replicate information to all DCs, so if a logon authentication fails due to a bad password, that DC will forward the authentication request to the PDC Emulator before rejecting the request.

When GPOs are updated, the group policy snap-in connects to the PDC emulator by default, reducing the possibility of overwriting GPOs.
There is one PDC Emulator per domain.

RID Master: The relative ID master allocates RIDs to each DC in the domain, in blocks of 512. RIDs are used to uniquely identify security principals, such as user, group and computer objects.
There is one RID Master per domain.

Infrastructure Master: The infrastructure master role is primarily designed for aiding multi-domain networks. When an object in one domain is referenced by an object in another domain, the object is referenced by the GUID, SID and distinguished name (DN). The job of the infrastructure master is to update the object's SID and DN in cross-domain references by querying the global catalog server for updates to the object in the other domain. The Infrastructure Master should not be a Global Catalog.
There is one Infrastructure Master per domain.

Global Catalog: Although not actually a FSMO role, GCs are necessary for the proper functionality of AD. GCs contain all commonly searched attributes for all objects in a forest. An attribute is included in the GC if the partialAttributeSet property of the attribute is set to true in the schema naming context.

Every DC in a forest can be a GC, but this is not a good idea, since GCs add a lot of overhead to a box and can cause problems with the Infrastructure Master FSMO role.

FSMO Role Locations

All FSMO Roles are maintained on the primary site.

DCKN1

- PDC Emulator
- RID Master
- Global Catalog

DCKN2

- Infrastructure Master,
- Domain Naming Master
- Schema Master

DCLA1 and DCOL1

Both are Global Catalogs, as is required for bridgehead servers.

Group Policy and Security

Basic Group Policy Implementation

Group Policy Overview

Group Policy Objects are a group of settings applied to a domain, site or OU, which allows control of policies, security, folder redirection, IE configuration and maintenance, logon and startup scripts, software publishing and assignment, and others. While local policies have been around since the Windows 95 days, they were not integral to the domain infrastructure, and the policies were never as expansive as they are now. With over 800 different configurable settings, security and configuration management without the use of group policy is an impossible task on a domain of any size.

Group Policies are split into User and Computer policy. User policy will be applied at logon to any computer a user logs on to successfully, while computer policy is applied at startup to the computer, and are effective for anyone logging on to the computer.

Policies are applied in order of local system, site, domain, and then top level OU on down to sub-OUs. Group Policy is applied in a “Last-Write Wins” configuration for each individual policy. This means that if a policy such as “Limit Profile Size” is enabled at the domain root level, but specifically disabled at the OU level, the end result of the policy is that the profile size is not limited on any machine in this OU. Although there are tools to help with the management of Group Policy, this is another reason it is important to limit complexity of the infrastructure only to what is truly necessary.

Group Policy best practices

When applying policies, GIAC has minded the following guidelines, which apply to a single domain, multi-site infrastructure from Microsoft's best practices on Group Policy deployment:

Disable unused parts of a Group Policy Object

If an OU that a Group Policy Object (GPO) is being applied to contains only users or only computers, the unused portion of policy should be disabled. This decreases startup and logon time for users and computers those policies are applied to. Since GIAC separates users and computers in most of its OUs, it takes full advantage of this

Use Block Policy and No Override sparingly

Blocking policy on an OU keeps higher level GPO's from being applied to that OU or any sub-OUs, while No Override keeps down-level OUs from blocking or overwriting policy applied in that GPO on down-level OUs. These functions can make it difficult to troubleshoot policy problems.

Minimize the number of GPOs associated with users in domains or OUs.

The more GPOs applied to a user, the longer it takes to process the policy at logon time. This is one of the reasons GIAC has such a flat OU structure.

Filter GPOs based on security group membership.

Users who do not have an Access Control Entry granting Apply rights to a GPO can avoid the logon delay, since policy will not be processed for those users.

Override user-based Group Policy with computer-based Group Policy only when necessary.

There is some overlap between user and computer policy. If these policies are applied in both the user policy and the computer policy, computer policy always overrides the user policy. This can cause difficulty in troubleshooting policy problems.

Users and computers are segmented in the AD by Organizational Units (OU). OUs are the primary method for applying Group Policies, although they can be applied to the root of the domain, sites scopes or individual computers as well. In the case of GIAC, OUs divide the users and computers up exclusively by job function.

The bold and italicized paths in the proceeding sections indicate the location for each set of bulleted items in the Group Policy MMC snap-in.

Default Domain Policy

GIAC has a carefully planned OU structure that doesn't require an advanced configuration from the default domain policy. The only policies applied to the default domain are the security settings which must be set at the root level of the domain, and policies which apply to all computers. Since these settings are computer specific, the user node of the GPO for the default domain is disabled. For the sake of clarity, all relevant settings will be listed. It will be specified if the setting used is the same as the default configuration.

Computer Configuration\Windows Settings\Security Settings\Account Policy\Password Policy

- "Enforce Password History" is set to 10 passwords remembered.
- "Maximum Password Age" is set to 90 days. Any more often would probably find a large number of users writing down their passwords instead of memorizing them.
- "Minimum Password Age" is set to 2 days. Combined with password history, this would keep a user from recycling the same password for a minimum of 20 days.
- "Minimum Password Length" is set to 9 characters. Users have been instructed on the use of passphrases whenever possible, so this limit is not too much of a burden.
- "Passwords must meet complexity requirements" is enabled. This requires that passwords use at least three of the four character types; upper case, lower case, number and special characters. Since most users are in fact using passphrases, and punctuation counts as special characters, this is again not much of an added burden on the users.

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

- "Account Lockout Duration" is set to 30 minutes, which is the default setting when enabled. Since anyone attempting a brute force attack would have to attempt a minimum of around 9^{72} (Uppercase possibilities + lower case possibilities + numerals, give or take a few thousand combinations), it is unfeasible for anyone to brute force an account password with any sort of account lockout. Even an internal attacker with a good idea what the password is would be unlikely to continue attempting to access an account when it unlocked every half hour, as it would be both time consuming and would most likely draw attention.
- "Account Lockout Threshold" was initially set to 3, as recommended in many documents, but several applications, including IE, were found to attempt failed logons 3 times in a row before prompting a user for password input. Lockout threshold was then set to 5.

- “Reset Account Lockout Counter After” is set to 30 minutes, which is the default configuration when enabled. The administrators saw no reason to change this.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- “Accounts: Administrator account status” is disabled. There is another local account, called Support, which is used if a machine is unable to authenticate against the domain and cached credentials cannot be used. Many scripts are designed to attack the local administrator account.
- “Accounts: Guest account status” is disabled (default).
- “Devices: Unsigned driver installation behavior” is set to “Warn, but allow installation”, instead of “Silently Succeed” which is the default for XP. This will warn users if a device driver is not signed as valid for the current operating system, making it easier for the helpdesk to troubleshoot problems.
- “Domain Member: Digitally encrypt secure channel data (always)” is enabled (default).
- “Domain Member: Require Strong (Windows 2000 or later) session key” is enabled. Clients will require 128-bit encrypted session keys.
- “Interactive logon: Do not display last user name” is disabled (default). This setting only marginally heightens security against a casual attacker with physical access to the system in question, and is inconvenient for end users.
- “Interactive logon: Do not require CTRL+ALT+DEL” is disabled. This policy is left not-configured by default, and if disabled on a machine could allow an attacker with physical access to the box to create a false logon screen on the machine in order to gather user names and passwords.
- “Interactive logon: Message text for users attempting to log on” is set to: “This is a private system owned by GIAC Corp. Only authorized users may log on to this computer. By logging on to this system, you agree to abide by all rules of computer conduct as outlined by company documentation, and agree to allow administrators and security staff to monitor your actions on this computer. If you are unwilling to comply with this message, you must leave this computer immediately”.
- “Interactive Logon: Message title for users attempting to log on” is set to: “Legal Warning”.
- “Microsoft network client: Digitally sign communications (always)” is enabled. This prevents the client from accepting SMB connections that are not digitally signed. This prevents man-in-the-middle attacks where SMB packets are modified in transit.

- “Microsoft network client: Digitally sign communications (if server agrees)” is enabled (default). This setting must remain enabled for the previous setting to take effect.
- “Network Access: Do not allow anonymous enumeration of SAM accounts and shares” is enabled. This prevents null-sessions from making connections and listing shares or user accounts on the local machine.
- “Network Security: Do not store LAN Manager Hash value on next password change” is enabled. The LAN Manager hash is used by LM and NTLM v1, and is a very weak hash. Disabling the LAN Manager hash in conjunction with user training on the use of passphrases makes password cracking almost impossible.
- “Network Security: LAN Manager authentication level” is set to “Send NTLMv2 response only” since all machines on the domain are NTLMv2 capable, and LM and NTLMv1 are insecure.

Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Computer

- The IP Filter list is set to require security for all connections. The primary option in the list requires SHA1 encrypted data integrity using AH. This is the configuration most servers are set to. The secondary option is configured as ESP with 3DES and SHA1 for connections to machines such as the HR & Financial file server.

Computer Configuration\Administrative Templates\System

- “Turn off Autoplay” is enabled for all drives. This prevents non-trusted media from running harmful executables automatically.

Computer Configuration\Administrative Templates\Network\Network Connections

- “Prohibit use of Internet Connection Sharing on your DNS domain network” is enabled
- “Prohibit installation and configuration of Network Bridge on your DNS domain network” is enabled

Default Domain Controller Policy

The default domain controller policy is applied to the Domain Controller OU. DCs are automatically added to this OU when they are created. The DC OU inherits policy from the root domain GPO by default, so many changes are already applied.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policies

The following settings have two options which can be configured: “Success” means that an entry will be placed in the Security log if the attempt is successful, and “Failure” means that an entry will be made in this log if the attempt fails. These settings must be made on the Domain Controllers GPO in order to monitor domain accounts and policies.

- “Audit Account Logon Events” is set to Success and Failure. This will monitor all attempted logons using domain accounts. This should be enabled in order to monitor for large numbers of failed attempts to access the network, or for large numbers of accesses from the same account.
- “Audit Account Management” is set to Success and Failure. This monitors any time someone tries to modify, create, or delete a domain account.
- “Audit Policy Change” is set to Success and Failure. This setting monitors attempts to change group policy for the domain.

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- “Add workstations to the domain” is set to Domain Admins and Support. The Authenticated Users group has been removed. This policy applies to all computer accounts in the domain, and must be applied to the Domain Controllers OU. It will be ignored if set in any other OU.
- “Allow logon through Terminal Services” is set to Administrators.
- “Logon locally” is set to Administrators.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- “Devices: Restrict CD-ROM access to locally logged-on user only” is enabled
- “Devices: Restrict floppy access to locally logged-on user only” is enabled
- “Devices: Unsigned driver installation behavior” is set to “Do not allow installation”. The DCs are all standard hardware, and should not have any unsigned drivers installed.
- “Interactive Logon: Do not display last user name” is enabled.
- “Interactive Logon: Smart Card removal behavior” is set to “Lock Workstation”.

- “Network Security: LAN Manager authentication level” is set to “Send NTLM v2 response only/ Refuse LM and NTLM”, since all clients are at least Windows 2000.
- “Shutdown: Clear virtual memory pagefile” is enabled. Under certain circumstances, if a DC is restarted with a floppy, sensitive data can be recovered from the system swap file.

Additional Group Policies

Each OU has its own GPO applied to it, although we won't go into detail on all of them here. The two most restrictive are the R&D and the R&D Servers.

R&D

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- “Deny access to this computer from the network” is set to Everyone. This keeps everyone from remotely accessing these machines using C\$ or remote registry. Since these are workstations, no file sharing should be done from these machines; all data should be stored on the file server.
- “Allow logon through Terminal Services” is empty. This disables the use of Remote Desktop to machines in this OU which are XP clients.
- “Logon Locally” is set to R&D Users and R&D Admins.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- “Interactive logon: Do not require CTRL+ALT+DEL” is disabled.
- “Interactive logon: Smartcard removal behavior” is set to “Lock Workstation”. All R&D user accounts are configured to require the use of smart cards.

Computer Configuration\Windows Settings\Security Settings\Local Policies\IP Security Policies on Local Computer

The Client policy has been applied in the following manner:

- A new filter has been created filtering all IP traffic to the 192.168.3.0 subnet. This is the subnet the R&D machines, including servers, are on. The filter requires that security be used, and only allows ESP with 3DES and SHA1 or MD5 to be used in communication with other machines on this subnet.

- The default filter is modified to require SHA1 AH authentication to all destinations.

SHA1 is stronger encryption than MD5, and has only marginally higher overhead. For this reason it was chosen as the AH authentication type.

Computer Configuration\Administrative Templates\Windows Components\Netmeeting

- “Disable remote Desktop Sharing” is enabled.

Computer Configuration\Administrative Templates\System\Remote Assistance

Note that this section applies to XP machines only. AD was updated with the XP policy files shortly after the XP rollout project started.

- “Solicited Remote Assistance” is disabled.
- “Offer Remote Assistance” is disabled.

Computer Configuration\Administrative Templates\Network\Offline files

- “Allow or Disallow use of the Offline Files feature” is disabled. This keeps users in the R&D group from utilizing offline files.

Computer Configuration\Administrative Templates\System

- “Turn off Autoplay” is enabled. This keeps CD-ROMs from attempting to run potentially malicious executables automatically when inserted into the drive.

User Configuration\Administrative Templates\Windows Components\Windows Installer

- “Prevent removable media source for any install” is enabled. This keeps R&D staff from installing software from a floppy or CD.

User Configuration\Administrative Templates\Windows Components\Windows Update

- “Remove access to use all Windows Update features” is enabled. This is not so much a security feature as a support feature. Too often, patches

from Windows Update marked 'critical' have caused application slowness or hangs. GIAC wants to control the timing of patch deployment.

User Configuration\Administrative Templates\Add-remove programs

Users in the R&D group are not allowed to install or modify components on their systems.

- "Hide the Add a program from CD-ROM or floppy disk option" is enabled.
- "Hide the Add programs from Microsoft option" is enabled.

User Configuration\Administrative Templates\Network\Network Connections

- "Prohibit TCP/IP advanced configuration" is enabled. Users have DHCP and should have no need of modifying their settings.
- "Prohibit access to the Advanced Settings item on the Advanced menu" is enabled. This keeps users from modifying their network bindings.
- "Prohibit adding and removing components for a LAN or remote access connection" is enabled. This keeps users from adding or removing bindings for network protocols such as TCP/IP.
- "Prohibit access to the New Connection Wizard" is enabled. Since there are no laptops in this OU, users do not need to create any remote access connections, and connections for network cards are created automatically.

User Configuration\Administrative Templates\System

- "Prevent access to registry editing tools" is enabled. This not only keeps users from editing the registry directly using regedit.exe and regedt32.exe, but also prevents editing the registry using a .reg file or by shelling out to regedit.

R&D Servers

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

Due to the sensitive nature of data on this server, it is important to monitor user access of data. Clearly, Administrators should be concerned if they see a high number of failed access requests, but they also need to watch for authorized users accessing much higher than normal numbers of files, or changing permissions on those files or directories.

- “Audit logon events” is set to Success and Failure. This will monitor attempts by users to connect to the R&D server.
- “Audit object access” is set to Success and Failure. This reports attempted access of individual files.
- “Audit privilege use” is set to Success and Failure. All attempts to modify permissions on files or directories will be reported.

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- “Access this computer from the network” is set to R&D Users and R&D Admins. This will prevent any other users from accessing this computer remotely.
- “Allow logon through Terminal Services” is set to R&D Admins.
- “Log on locally” is set to R&D Admins.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- “Accounts: Administrator Account Status” is disabled.
- “Devices: Unsigned driver installation behavior” is set to disallow installation.
- “Interactive logon: Smartcard removal behavior” is set to “Lock Workstation”.
- “Network Security: Lan Manager authentication level” is set to “Send NTLM v2 response only/refuse LM and NTLM”, since all clients on the domain are Windows 2000 or newer.
- “Shutdown: Clear memory pagefile” is enabled.

Computer Configuration\Windows Settings\Security Settings\Local Policies\IP Security Policies on Local Computer

The “Secure Server (Require Security)” policy has been applied. This requires that all communication between any machine on the network and the machines in the R&D Servers OU be encrypted. The policy is applied in the following manner:

- No new rules need to be created. The All IP Traffic rule is modified to only accept ESP with 3DES SHA1 or 3DES MD5.

Computer Configuration\Administrative Templates\Windows Components\Terminal Services

- “Limit users to one remote session” is enabled. This keeps Admins from logging on remotely to these servers from more than one location.
- “Remote Control settings” are enabled, and set to “No Remote Control allowed”. This keeps anyone from viewing a currently running Terminal Services session.

Note that it is not necessary to limit total number of connections, since Terminal Services is configured in Remote Administration mode, which limits the server to two simultaneous sessions.

Computer Configuration\Administrative Templates\System

- “Turn off Autoplay” is enabled.
- “Download missing COM components” is disabled. This keeps the server from searching for components whose use is being attempted, but which are not installed on the machine.

Additional Security measures**Physical Security**

Physical security of Windows Servers and Admin Machines is especially important since it is almost impossible to maintain security on a machine which has been physically compromised.

All DCs and non-R&D servers, including HRs, are kept in a locked room in the main office. The main offices have a receptionist at the front entrance to monitor access to the building and the only people with access to this room are the Domain Admins and the facilities administrator. Anyone accessing this room can only do so with the escort of someone with access to the server room.

The dropped ceiling extent in most of the offices has been removed from this room to ensure that no one can access the room by climbing through the ceiling. The servers are elevated from the floor and covered by a rack in order to protect them from water damage. The racks containing the servers and backup devices are locked at all times, and all servers are hooked to a UPS.

User and workstation naming conventions

One common method for naming computers and user accounts is to use a derivation of the user's full name for either user or computer account or both. This is a sloppy method, since obtaining the full names of support staff is a

relatively trivial exercise. Once obtained, for most social engineers, this makes the process of determining which computers to attack trivial as well. Users are assigned a random 5-digit user ID with a letter prefix, depending on type of access allowed. 5 digits was thought to be enough to cover any future expansion by the company, while being short enough to be easily remembered. A random number was chosen to keep attackers from easily guessing login IDs.

An account with a “U” prefix denotes standard user access, while “S” and “A” accounts denote special and admin accounts, respectively. For example, a standard user account might be U27084. All users with S and A accounts also have normal U accounts. Special and Admin accounts are not to be used to directly log on to desktop machines, but should only be used in conjunction with the “Run As” feature, so as to limit the total number of applications running in this context. In addition, S and A accounts are explicitly denied access to the internet, and do not have email accounts assigned to them. Since almost all viruses are obtained from email or internet sites, this limits the possibility of a user logged on with special privileges getting infected. Most A accounts are in the Domain Admins security group.

Workstations are denoted by a zero-filled six-digit requisition number, prefixed with WS to denote “workstation”. A typical workstation account might be WS000794.

Password Reset and Privileged Resource Access

Only a small number of the helpdesk staff is permitted to reset passwords for general users. This staff has been instructed to request the birthday and badge number of the employee requesting their password reset. This data is checked against the privileged information available on this user in AD. If the information is incorrect or the user cannot provide their badge number, the helpdesk is not to provide any further information to the user and should get off the phone immediately.

When access to network resources, such as printers or shares, is requested, the access request must be verified with the resource owner. The resource owner may call the helpdesk directly and provide badge number and birthday or may send an email detailing the request to helpdesk@giac.int.

Wireless and VPN access

Wireless and VPN access are allowed only in the Kennewick location, and are handled very similarly in the GIAC domain.

GIAC has a large number of traveling salespeople who connect remotely for mail and resource access on a regular basis, and the factory supervisors need access to their monitoring equipment from anywhere on the floor.

Both Access Points (APs) and the VPN concentrator are configured as Network Access Clients (NAS). Each NAS is set up on an un-trusted subnet, and authenticates requests against the IAS server inside the network.

Both "S" and "A" accounts have been disallowed access to the network remotely, although once connected to a terminal server, they can use the "Run As" function to do any required work.

Certificates

Certificates are required on this domain for the use of un-trusted access such as wireless and VPN, as well as for smartcard users.

The root Certificate Server is on a removable hard drive which is only connected when creating new subordinate certificate servers. There is only one issuing CA on the network CAKN2, which is located at the Kennewick site.

© SANS Institute 2003, Author retains full rights.

References

Infrastructure Master and Global Catalog

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADgcInfFSMO.htm

Dcpromo.exe Does Not Work if the Domain Naming Master Is Not a Global Catalog

<http://support.microsoft.com/default.aspx?scid=kb;en-us;315850>

Group Policy best practices

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_sp_bestprac.htm

Performance comparison of MD5 vs SHA1

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbda/html/bdadotnetarch15.asp>

MOC 2154, Implementing and Administering Microsoft Windows 2000 Directory Services. Redmond: Microsoft Press, 1999.

MOC 2150, Designing a Secure Microsoft Windows 2000 Network Redmond: Microsoft Press, 1999.

Shinder, Thomas W. et. al. ISA Server and Beyond. Syngress, 2002

Fossen, Jason. Securing Windows